DICKINSON WRIGHT PLLC
JOHN P. DESMOND
Nevada Bar No. 5618
JUSTIN J. BUSTOS
Nevada Bar No. 10320
100 W. Liberty Street, Suite 940
Reno, NV 89501
Tel: 702-550-4400
Fax: 844-670-6009
Email: jdesmond@dickinsonwright.com
Email: jbustos@dickinsonwright.com

(Additional counsel listed on signature page)

Attorneys for Defendant Ozone Networks, Inc. d/b/a OpenSea, a New York Corporation

UNITED STATES DISTRICT COURT
DISTRICT OF NEVADA

ROBERT ARMIJO, Plaintiff, vs. OZONE NETWORKS, INC. d/b/a OPENSEA, a New York Corporation, YUGA LABS, LLC d/b/a BORED APE YACHT CLUB, a Delaware limited liability company, LOOKSRARE; and DOES 1 to 50, Defendants.	CASE NO. 3:22-CV-00112-MMD-CLB **DEFENDANT OZONE NETWORKS, INC.'S MOTION TO DISMISS COMPLAINT**

Defendant Ozone Networks, Inc. d/b/a OpenSea, by and through its counsel of record, Munger, Tolles & Olson LLP and Dickinson Wright PLLC, hereby submits its Motion to Dismiss Complaint ("Motion"). This Motion is made pursuant to Fed. R. Civ. P. 12(b)(6) and is supported by the attached Memorandum of Points and Authorities, the concurrently filed Request for Judicial Notice and Declaration of Ian L. Meader, all papers and pleadings on file herein, and any oral argument this Court chooses to consider.

TABLE OF CONTENTS

TABLE OF AUTHORITIES

PAGE(S)

FEDERAL CASES

TABLE OF AUTHORITIES
(CONTINUED)

PAGE

TABLE OF AUTHORITIES
(CONTINUED)

PAGE

TABLE OF AUTHORITIES
(CONTINUED)

PAGE

MEMORANDUM OF POINTS AND AUTHORITIES

I. INTRODUCTION

Ozone Networks, Inc. d/b/a OpenSea ("OpenSea") operates a web3 peer-to-peer marketplace where users can explore non-fungible tokens ("NFTs"), and can connect directly with each other to purchase and sell NFTs. NFTs are uniquely identifiable digital items, representing ownership in digital art, music, and collectibles. NFTs "live" (that is, they are custodied) on "blockchains." Blockchains are distributed digital ledgers that, among other things, record the ownership of NFTs. OpenSea only displays NFTs from public blockchains—meaning blockchains that anyone can interact with to view, buy, sell, or transfer NFTs.

Although NFTs are relatively novel, the legal issues presented in this case are not. Plaintiff Robert Armijo alleges that although he *purchased* three NFTs using OpenSea's platform, these NFTs were subsequently stolen through a phishing scam by a third party on a completely different online platform—Discord—that is not affiliated with OpenSea in any way. (Compl. ¶¶ 46-47, ECF No. 1; *id.* ¶ 52 ("[T]he theft did not occur on OpenSea's platform.").) Plaintiff asserts that OpenSea is nevertheless liable for the loss of his stolen NFTs enabled by his use of the unaffiliated Discord platform because, he alleges, OpenSea owed and breached a duty to prevent the third party from subsequently relisting those NFTs for sale on its platform.

That is not the law. Indeed, far from presenting any novel legal questions, it has long been the rule in Nevada that "no duty is owed to control the dangerous conduct of another or to warn others of the dangerous conduct, except where a special relationship exists and the harm is created by foreseeable conduct." *Beckman v. Match.com, LLC*, No. 2:13-CV-97 JCM (NJK), 2017 WL 1304288, at *3 (D. Nev. Mar. 10, 2017) (*Beckman I*), *aff'd*, 743 F. App'x 142 (9th Cir. 2018) (Mem. Disp.) (*Beckman II*). "Nevada courts have never recognized a special relationship akin to that between" a website and its users. *Beckman II*, 743 F. App'x at 142 (no duty for Match.com to protect subscribers from third parties). Because there was no duty owed to Plaintiff, his claim for negligence against OpenSea is a nonstarter.

Even if such a special relationship *did* exist between Plaintiff and OpenSea, Plaintiff does not plausibly allege that OpenSea breached any purported duties to Plaintiff or that its actions caused him any harm. First, Plaintiff acknowledges that because OpenSea acted within a matter of hours to disable the ability to buy, sell, or transfer the NFTs using OpenSea's services, two of the three NFTs stolen via a third party on the Discord platform were never resold using OpenSea. The third NFT was resold just two hours after the theft via the Discord platform. (Compl. ¶¶ 60-62, ECF No. 1.) Second, Plaintiff did not suffer any harm *caused by OpenSea* from this resale because, as the Complaint alleges, the theft of Plaintiff's NFTs became "permanent and irreversible" the instant the phishing scam Plaintiff fell prey to on the Discord platform was complete. (*See id.* ¶ 4.) Plaintiff's own allegations explain that OpenSea is powerless to "undo a transaction once it has been completed on the blockchain" or "prevent the stolen NFTs from being purchased or traded on any other NFT marketplaces" other than OpenSea—which is exactly what happened with two of the stolen NFTs. (*Id.* ¶¶ 4, 61.)

Plaintiff's claims for negligent hiring, training, and supervision are substantively duplicative of his negligence claim, and are similarly flawed. As with his negligence claim, Plaintiff does not allege that *OpenSea's employees* caused him harm—only that their steps to remediate harm caused by an unaffiliated third party who had stolen his NFTs through a phishing scam on another platform were inadequate. "It is a basic tenet that for an employer to be liable for negligent hiring, training, or supervision of an employee, the person [causing the harm] must actually be an employee," not a third party. *Rockwell v. Sun Harbor Budget Suites*, 925 P.2d 1175, 1181 (Nev. 1996).

Finally, all of Plaintiff's claims are separately barred both by contract and by the economic loss doctrine. First, Plaintiff agreed to OpenSea's Terms of Service, which clearly and unambiguously disclaim liability for negligence claims focused on harms caused by third parties, including injuries related to "phishing." *See Kaufman v. Sweat It Out, Inc.*, No. A-18-778889-C, 2020 WL 4251083, at *3 (Nev. Dist. Ct. June 17, 2020) ("The exculpatory clause unambiguously identifies the parties' intent; and therefore, the Court has no authority to alter the

terms of the Agreement."); *Cruz v. Sun Buggy Fun Rentals, Inc.*, No. 11A652884, 2012 WL 7831781 ¶¶ 6, 9 (Nev. Dist. Ct. Nov. 19, 2012) (exculpatory provision enforceable when customers "simply can walk away"). Second, all of Plaintiff's claims are barred by Nevada's economic loss doctrine because they seek damages that are solely monetary in nature. "Under the economic loss doctrine . . . economic losses are not recoverable in negligence absent personal injury or damage to property other than the defective entity itself," neither of which Plaintiff alleges here. *Calloway v. City of Reno*, 993 P.2d 1259, 1267 (Nev. 2000), *overruled on other grounds by Olson v. Richard*, 89 P.3d 31, 33 (Nev. 2004).

For each of these reasons, Plaintiff's Complaint against OpenSea should be dismissed, and because these issues cannot be addressed by amendment, the dismissal should be without leave to amend.

II. FACTUAL AND PROCEDURAL BACKGROUND

A. The OpenSea Marketplace and the NFT Community

As alleged in Plaintiff's Complaint, NFTs are "uniquely identifiable digital assets" representing ownership in digital art, music, collectibles, and other digital properties. NFTs "live" (that is, they are custodied) on a blockchain—a digitally distributed, decentralized, public ledger. (Compl. ¶ 2, ECF No. 1; *id.* ¶ 4 ("Whenever an NFT changes hands, the underlying blockchain technology creates a public record of the transaction on its digital ledger.").) NFTs, like cryptocurrencies, are stored by their owners using digital "wallets." (*Id.* ¶ 4.)

OpenSea is a web3 peer-to-peer NFT marketplace where users can find NFTs that interest them and connect with each other to purchase and sell NFTs. The NFT community is much larger than OpenSea, however. (*Id.* ¶¶ 7, 21.) For example, there are many other NFT platforms where NFTs can be bought and sold—including LooksRare, which is also a named defendant in this case. (*Id.* ¶ 62.) And, as Plaintiff alleges, the "NFT community primarily communicates through two platforms: Twitter and Discord." (*Id.* ¶¶ 22, 23 ("Discord is an online communications app that serves as a semipublic, forum-style community platform.").) Further, because OpenSea allows users to buy and sell NFTs using cryptocurrency but does not

allow users to trade or exchange NFTs for other NFTs, "consumers often use Discord's NFT servers to . . . set up NFT trades through third-party NFT trading websites." (*Id.* ¶ 26.)

The Complaint alleges that it is well-known in the NFT community that "NFTs have become a booming target for scams and theft," and that platforms like Discord are "easily accessible to bad actors and [are] rife with phishing scams and malicious hacking." (*See id.* ¶¶ 27, 84.) Because OpenSea takes the security of its platform and its users extremely seriously, it routinely warns users about the significant security risks involved in holding and trading NFTs and provides recommendations for how to address such risks—including, for example, offering what Plaintiff characterizes as a "memorable recommendation" that consumers should "use an 'air-gapped' computer when viewing their digital wallets to achieve the highest level of security. An air-gapped computer is one that has never been connected to the internet," and certainly never used to access the online Discord platform. (*See id.* ¶ 7.)

OpenSea also warns its users about the risks associated with NFTs in its Terms of Service, which all users must accept to use the platform. (*See* Declaration of Ian L. Meader ("Meader Decl.") Ex. A at 12 (disclosing "the risk that third parties may obtain unauthorized access to information stored within your wallet").)[1] The Terms of Service also contain express limitations of liability, providing that OpenSea "WILL NOT BE RESPONSIBLE OR LIABLE TO YOU FOR . . . ANY LOSSES, DAMAGES OR CLAIMS ARISING FROM . . . ANY UNAUTHORIZED THIRD PARTY ACTIVITIES, INCLUDING WITHOUT LIMITATION . . . PHISHING," and further providing that the user agrees that "IN NO EVENT WILL OPENSEA BE LIABLE TO YOU OR ANY THIRD PARTY FOR ANY . . . DAMAGES . . . WHETHER CAUSED BY," *inter alia*, "TORT (INCLUDING NEGLIGENCE)." (*Id.* at 11-12.)

Plaintiff agreed to OpenSea's Terms of Service on multiple occasions, including when he purchased NFTs using OpenSea and used the mobile app for the first time. (Meader Decl. ¶¶ 5-8; *see* Compl. ¶¶ 28, 32, ECF No. 1.) In doing so, Plaintiff was at least twice required to check a

[1] As set forth in its Request for Judicial Notice, OpenSea requests that the Court take judicial notice of the Terms of Service, which are incorporated by reference into the Complaint.

box next to the statement that, "By checking this box, I agree to OpenSea's Terms of Service," which contained a hyperlink to OpenSea's Terms of Service. (Meader Decl. ¶¶ 6-8.)

B. Plaintiff Fell Victim To a Third-Party Phishing Attack on a Different Platform

This is not a case "where hackers employ[ed] complicated high-level techniques to find and exploit weaknesses in [OpenSea's] computer code." (Compl. ¶ 10, ECF No. 1.) In fact, the phishing attack to which Plaintiff fell prey did not occur on the OpenSea platform at all—as Plaintiff acknowledges, it happened on Discord, a third-party platform. (*See id.* ¶¶ 46-52.)

Between November 2021 and January 2022, Plaintiff purchased a "Bored Ape" NFT and two "Mutant Ape" NFTs. (*Id.* ¶¶ 30-32.) In February 2022, he accessed a Discord server associated with a collection of NFTs called "Cool Cats" with the goal of trading one of his NFTs for a "Cool Cats" NFT. (*Id.* ¶ 46.) Plaintiff reached an agreement on terms for such a trade with another user on Discord and—because NFTs cannot be traded using the OpenSea platform—proposed to execute the trade on a third-party website called "NFT Trader." (*Id.* ¶ 47.)

The other Discord user agreed, and sent Plaintiff a link to what appeared to be the "NFT Trader" website—despite having claimed just "a few minutes" earlier that he "had never heard of or used NFT Trader before." (*Id.* ¶¶ 47-48.) Unfortunately, when Plaintiff followed the link and then clicked another link to approve the trade, he fell victim to a "phishing" attack. (*Id.* ¶¶ 49-51 ("The link [the attacker] had sent was actually connected to a fake website made to look like the real NFT Trader site.").) When Plaintiff clicked the link to approve the trade, the other Discord user (the attacker) gained access to the NFTs that are the subject of this Complaint and transferred them to his own wallet. (*Id.*) As Plaintiff alleges, the NFTs at that point were irretrievably stolen. (*See id.* ¶ 4 (NFT transactions "become[] permanent and irreversible" after they have "been completed on the blockchain").)

C. OpenSea Took Immediate Action, but NFT Theft Is Irreversible

"Although the theft did not occur on OpenSea's platform, [Plaintiff] suspected that the thief would list the stolen NFTs on OpenSea to try and sell them as quickly as possible." (*Id.*

¶ 52.) Plaintiff sent a series of messages to OpenSea customer service, and its customer service representatives acted promptly (within four hours) to prohibit further purchase or sale of the NFTs using OpenSea. (*Id*. ¶ 61.) OpenSea's prompt action thwarted the attacker from ever reselling using the OpenSea platform two of the three NFTs stolen from Plaintiff; the third NFT was resold using OpenSea approximately two hours after the theft occurred via the Discord platform. (*Id.* ¶¶ 60-62 (sole resale using OpenSea took place "approximately two hours after the theft").)

Due to the decentralized nature of blockchain technology, however, freezing the purchase or sale of the NFTs using OpenSea does "not prevent the stolen NFTs from being purchased or traded on any other NFT marketplaces." (*Id.* ¶ 61.) And that is exactly what happened—"[f]ollowing the freeze of the NFTs on OpenSea's marketplace," *i.e.*, following OpenSea's prompt action, the other two "NFTs were later listed and resold on LooksRare," a different NFT platform. (*Id.* ¶ 62 (noting that one of the three NFTs has resold more than once on LooksRare).)

D. Plaintiff's Allegations Against OpenSea

Plaintiff filed the instant action on February 28, 2022, against OpenSea, LooksRare (which never froze listings of Plaintiff's NFTs), and the makers of the "Bored Ape" and "Mutant Ape" NFT collections, Yuga Labs, LLC (d/b/a the Bored Ape Yacht Club ("BAYC")). (*See id*. ¶¶ 6-8.) In brief, Plaintiff alleges that OpenSea failed to "monitor[] [its] NFT marketplace[] for stolen NFTs" and "utilize[] an approval process to screen NFTs prior to listing them on the OpenSea marketplace" to "combat abuse," and to prevent the stolen NFTs at issue from being listed on OpenSea. (*Id*. ¶¶ 124, 98-99; *see also id.* ¶ 60 (complaining that Plaintiff's "Bored Ape NFT #4319 was listed for sale on OpenSea"); *id.* ¶ 66 (thieves "unloaded the stolen goods by immediately listing and selling them on OpenSea").) Plaintiff brings claims against OpenSea for (1) negligence; (2) negligent supervision and training; and (3) negligent hiring. (*Id.* ¶¶ 1, 13, 123-136, 146-165.) Plaintiff alleges that he was harmed by the loss of the "significant monetary value of the NFTs" as well as the "commercialization rights he possessed" in the NFT images and his "ability to earn future profits from his BAYC NFTs." (*Id.* ¶¶ 114, 134, 143, 154.)

III. LEGAL STANDARD

"To survive a motion to dismiss" pursuant to Rule 12(b)(6), "a complaint must contain sufficient factual matter, accepted as true, to 'state a claim to relief that is plausible on its face.'" *Ashcroft v. Iqbal*, 556 U.S. 662, 678 (2009) (quoting *Bell Atl. Corp. v. Twombly*, 550 U.S. 544, 570 (2007)). "[L]egal conclusions are not entitled to the assumption of truth," and "[m]ere recitals of the elements of a cause of action, supported only by conclusory statements, do not suffice." *Cincinnati Specialty Underwriters Ins. Co. v. Red Rock Hounds*, 511 F. Supp. 3d 1105, 1113 (D. Nev. 2021) (citing *Iqbal*). "When the claims in a complaint have not crossed the line from conceivable to plausible, the complaint must be dismissed." *Id.* (citing *Twombly*).

IV. ARGUMENT

Plaintiff fails to state a claim as to any of his three substantively identical causes of action for negligence. Each of the three claims is also barred by contract—the liability limitations in the OpenSea Terms of Service, to which Plaintiff repeatedly agreed—and by the economic loss doctrine.

A. Plaintiff Fails to State a Claim For Negligence

Plaintiff's allegations against OpenSea fail to establish three of the four elements of negligence. "A plaintiff alleging negligence must demonstrate '(1) the existence of a duty of care, (2) breach of that duty, (3) legal causation, and (4) damages.'" *Sparks v. Alpha Tau Omega Fraternity, Inc.*, 255 P.3d 238, 244 (Nev. 2011). Plaintiff fails to allege the existence of a duty, any breach of that duty, or legal causation.

1. OpenSea Had No Duty To Protect Plaintiff From Harm By Third Parties

Plaintiff contends that OpenSea violated a duty to monitor its platform and react more quickly to aid users in preventing the listing of NFTs stolen by third parties. No such duty exists.

"Under Nevada law, no duty is owed to control the dangerous conduct of another or to warn others of the dangerous conduct, except where a special relationship exists and the harm is created by foreseeable conduct." *Beckman I*, 2017 WL 1304288, at *3. Plaintiff plainly

acknowledges that the theft of his NFTs was, as stated in *Beckman I*, the fault "of another," alleging that "the theft did not occur on OpenSea's platform and was executed by a third party with no relation to OpenSea" (Compl. ¶¶ 46-47, 52, ECF No. 1), but does not offer even a conclusory allegation that a special relationship existed here between himself and OpenSea; he alleges only that OpenSea "owed a duty to Mr. Armijo as a NFT consumer to exercise reasonable care" (*id*. ¶ 124). This alone renders Plaintiff's allegations insufficient, warranting dismissal of his negligence claim. *Beckman I*, 2017 WL 1304288, at *3 ("As mere recitation of the elements is insufficient to substantiate a claim, the court finds that [plaintiff] has not sufficiently pleaded the element of duty.")

Nor could Plaintiff's factual allegations be bootstrapped into a finding that such a special relationship exists. "[T]he pivotal factor in the determination of liability arising from" a special relationship is "the element of control" over the harmed party—here, control over Plaintiff. *Scialabba v. Brandise Const. Co.*, 921 P.2d 928, 930 (Nev. 1996) (special relationships include "landowner-invitee, businessman-patron, employer-employee, school district-pupil, hospital-patient, and carrier-passenger"). When one party has control over another, that party may have a duty to protect the controlled party because "the ability of [the controlled party] to provide for his own protection has been limited in some way by his submission to the control of the other." *Sparks*, 255 P.3d at 244-45 (quoting *Scialabba*, 921 P.2d at 930). Conversely, where the defendant does not have control, or when the plaintiff's ability to provide for their own protection has not been limited to submission to control, there is no special relationship. *Compare Sparks*, 255 P.3d at 245 (fraternity had no duty to protect from harm by third party outside area under its control), *with Scialabba*, 921 P.2d at 931 (contractor "responsible for locking the doors" owed duty to protect against harm by third parties).

Courts consistently hold as a matter of law that websites and other online platforms do not have a "special relationship" with their users. In a case comparable to this one, the Ninth Circuit upheld dismissal under Nevada law of a plaintiff's claim against the subscription dating website Match.com for negligence based on allegations that she was "viciously attacked" by a

third party with whom she was matched by the website—noting that "Nevada courts have never recognized a special relationship akin to that between" Match.com and its users. *Beckman II*, 743 F. App'x at 142. Explaining that the ability to control "must be able to 'meaningfully reduce the risk of harm that actually occurred'" to give rise to a special relationship, the district court opinion affirmed by the Ninth Circuit held that the plaintiff's "ability to protect herself was not limited in any way by submission to the control of another." 2017 WL 1304288, at *3.

Likewise, in a case similar to this one involving fraud perpetrated by a third party, the Second Circuit cited the Ninth Circuit's decision in *Beckman* to support its conclusion that the online payment processing site PayPal was not in a special relationship with its users and thus did not owe a user a duty to monitor and investigate fake accounts created by a third party with unauthorized access to the user's information. *Bibicheff v. PayPal, Inc.*, 844 F. App'x 394, 397 (2d Cir. 2021) (summary order) (holding that the plaintiff's "injury was a result of [a third party's] access to her personal and business information, including credit card information – access used by the [third party] to defraud [the plaintiff], but for which PayPal is not alleged to have been responsible").

And in *Dyroff v. Ultimate Software Grp., Inc.*, 934 F.3d 1093 (9th Cir. 2019), the Ninth Circuit held that a social media website did not have a special relationship with a user and had no duty to warn or protect the user against a third party who sold drugs to the user—drugs which resulted in the user's fentanyl overdose and death. The Ninth Circuit reached this conclusion even though "[s]ome of the site's functions, including user anonymity and grouping," and user content recommendations, "facilitated illegal drug sales." *Id.* at 1094-95. The Ninth Circuit emphasized that "[n]o website could function if a duty of care was created when a website facilitates communication, in a content-neutral fashion, of its users' content. . . . We decline to create such a relationship." *Id*. at 1101 (applying comparable California law); *see also Dyroff v. Ultimate Software Grp., Inc.*, No. 17-CV-05359-LB, 2017 WL 5665670, at *14 (N.D. Cal. Nov. 26, 2017) (trial court decision citing *Beckman I* to support the "conclusion that a website has no 'special relationship' with its users").

Several other courts across the country have held similarly. *See, e.g.*, *Klayman v. Zuckerberg*, 753 F.3d 1354, 1359-60 (D.C. Cir. 2014) (no special relationship between Facebook and its users); *Ginsberg v. Google Inc.*, __ F. Supp. 3d __, No. 21-CV-00570-BLF, 2022 WL 504166, at *8 (N.D. Cal. Feb. 18, 2022) (holding that Google's guidelines for app developers do not give rise to duty to protect Android users from hate speech); *Carroll v. Am. Empire Surplus Lines Ins. Co.*, 289 F. Supp. 3d 767, 774 (E.D. La. 2017) (holding that "Airbnb did not owe Plaintiffs a duty" to protect them from injuries on hosts' properties "because of a special relationship between Plaintiffs and Airbnb").

The same result is compelled here. Plaintiff's proposal that the Court find a "duty" for OpenSea to protect Plaintiff from harm by a third party through monitoring its platform for listings of stolen NFTs and removing such listings (*see* Compl. ¶ 124, ECF No. 1) is indistinguishable from the duties proposed and consistently rejected, again and again, in this line of case law. *E.g.*, *Beckman II*, 743 F. App'x at 142 (no duty to warn users that another user might be dangerous); *Bibicheff*, 844 F. App'x at 397 (no duty to monitor and investigate fake accounts used to commit fraud); *Dyroff*, 934 F.3d 1093, 1101 (no duty to warn users about another user's criminal activity). Plaintiff's allegations establish that his ability to protect himself "was not limited in any way by submission to" OpenSea's control—control which Plaintiff's own allegations demonstrate is nonexistent. *Beckman I*, 2017 WL 1304288, at *3.

Indeed, the alleged facts here starkly demonstrate the absence of any conceivable duty by OpenSea to protect Plaintiff from third-party harm. Plaintiff's claim to such a duty is even weaker than the basis for the duties proposed in many of the cases cited above, such as *Beckman* and *Dyroff*, where the wrongdoer connected with the injured plaintiff on the defendant's platform. Here, by contrast, the wrongdoer and Plaintiff connected and the attack took place on a Discord server hosted by third parties over which OpenSea plainly had no control. (Compl. ¶¶ 46-47, ECF No. 1 (Plaintiff sought to negotiate trade using the third-party "Cool Cats Discord server," not OpenSea; and then sought to consummate a trade on "a third-party NFT trading website" called "NFT Trader," not OpenSea); *cf. id.* ¶¶ 26-27 ("[C]onsumers often use Discord's

NFT servers" to arrange trades even though "the platform is easily accessible to bad actors and is rife with phishing scams and malicious hacking" because OpenSea "only allow[s] customers to buy or sell NFTs," not to trade them).) This alone warrants dismissal of Plaintiff's claims.

Additionally, resale of two of the three stolen NFTs occurred using the LooksRare platform, not OpenSea. (*Id.* ¶ 62.) OpenSea owes no duty to protect against harm from third parties on Discord or LooksRare, areas entirely outside its control. *Beckman I*, 2017 WL 1304288, at *3 (holding that even if plaintiff could show that Match.com paired her with the third party in the first instance, "the claim would still fail because the brutal attack occurred offline several months" later); *Sparks*, 255 P.3d at 245 (no duty to protect from third-party harm outside area of control).

More broadly, as an NFT marketplace, OpenSea had *zero* control over Plaintiff's NFTs themselves, and its limited control over listings posted using its own platform of NFTs does not establish a special relationship as a matter of law. Like all OpenSea users, Plaintiff held his NFTs on the blackchain using his own digital wallet—not in the custody of OpenSea—and he was free to transfer or sell his NFTs on any platform he wished. (Compl. ¶ 4, ECF No. 1 (alleging that "digital wallets" are "the software-based system used to hold the NFTs"), *id.* ¶ 28 (alleging that "Mr. Armijo also set up a digital wallet with MetaMask, an online service that houses software-based digital wallets that allow users to store their digital assets.").)

The subsequent transactions using another marketplace alleged here demonstrate the sharply circumscribed limits of OpenSea's purported "control" over anything: OpenSea cannot limit transactions using other platforms because it does not have any control over those platforms or the decentralized blockchain technology underlying NFTs. (*Id.* ¶¶ 61-62.) And although (like any other website) OpenSea can monitor or prohibit listings on its own platform, not only would that not have prevented the resale of Plaintiff's NFTs elsewhere (in other words, resales on LooksRare or another platform would still go forward), but the law is well-settled that such routine website operations are insufficient as a matter of law to establish the existence of a special relationship and a duty. *E.g., Beckman II*, 743 F. App'x at 142 (no special relationship

between website and user where website allegedly had unique access to information about users and used that data to create "matches" between users); *Dyroff*, 934 F.3d at 1101 (no special relationship between website and user where website used an algorithm to generate and offer "recommendations and notifications" to users based on their activities and preferences).

Lastly, the policy consequences of creating a new duty for online platforms like OpenSea to protect their users from harm by third parties would be severe. The full scope of the duties Plaintiff alleges is breathtaking: he would require OpenSea not only to eliminate all listings for any NFT that any user reported stolen within seconds and without investigation, but even to be deputized by law enforcement to help retrieve such NFTs. (*See, e.g.*, Compl. ¶ 12, ECF No. 1 (alleging duties to "monitor its community of legitimate owners," "restrict access of NFTs that are known to be stolen," "aid victims whose BYAC NFTs were stolen," and "assist law enforcement officials in attempts to retrieve stolen NFTs").) As the Ninth Circuit has observed, creating such expansive, unbounded duties could effectively prohibit online platforms from functioning. *Dyroff*, 934 F.3d at 1101 ("No website could function if a duty of care was created when a website facilitates communication, in a content-neutral fashion, of its users' content.").

2. Even If OpenSea Did Have Such a Duty, Its Actions Did Not Constitute a Breach

Plaintiff contends that OpenSea had a duty to "exercise reasonable care in providing adequate customer service for victims of theft or other illegal activities that occurred *on [its] platform[]*" and in "monitoring [its] NFT marketplace[] for stolen NFTs." (Compl. ¶¶ 124-125, ECF No. 1.) As explained above, OpenSea owed no such duty—but even if it did, its actions did not constitute a breach.

First, Plaintiff readily admits that "the theft did not occur on OpenSea's platform" and does not allege that OpenSea is responsible in any way for the phishing attack that enabled the theft of his NFTs. (*Id.* ¶ 52; *see id.* ¶ 7 (OpenSea routinely warns users about the risks of third-party attacks and has taken "high-level technological measures" to stop "complicated computer hacking and malicious software attacks"); *id.* ¶ 10 (contrasting this case with "NFT theft cases

where hackers employ complicated, high-level techniques to find and exploit weaknesses in a platform's computer code").) As set forth above, it is indisputable that the theft itself took place entirely on platforms outside of OpenSea's control—the unaffiliated Discord platform and the (fake) third-party "NFT Trader" website—and OpenSea had nothing to do with the theft itself.

Second, Plaintiff also admits that OpenSea took prompt action within hours to disable the listings on OpenSea, and that two of the three stolen NFTs have never been resold using OpenSea. (*Id.* ¶ 62 ("Following the freeze of the NFTs on OpenSea's marketplace," two "NFTs were later listed and resold on LooksRare.").) Thus, even if Plaintiff could plead a special relationship with OpenSea sufficient to give rise to a duty to control listings of stolen NFTs, Plaintiff himself alleges that OpenSea indisputably acted consistent with that purported duty with respect to two of the three NFTs at issue.

Third and finally, with respect to the one NFT that was resold a single time using OpenSea within *just two hours* of Plaintiff falling victim to the phishing attack on the Discord platform and the (fake) third-party "NFT Trader" website, and before OpenSea could take action, Plaintiff does not and cannot plausibly allege breach of his proposed duty. (*Id.* ¶¶ 60-61 (OpenSea froze NFTs within four hours).) OpenSea's expeditious action does not constitute a breach of the (nonexistent) duty Plaintiff alleges. *See, e.g.*, *Ripple Labs Inc. v. YouTube LLC*, No. 20-CV-02747-LB, 2020 WL 6822891, at *4 (N.D. Cal. Nov. 20, 2020) (holding that YouTube is not liable for trademark infringement when it took down videos that mark holder alleged were infringing within "a week, several weeks, around two months"); *Acad. of Motion Picture Arts & Scis. v. GoDaddy.com, Inc.*, No. CV 10-03738 AB (CWX), 2015 WL 5311085, at *10, 35 (C.D. Cal. Sept. 10, 2015) (GoDaddy "quickly responded" and acted "promptly upon receipt of any complaint," *i.e.*, "[o]n average . . . within 2.75 days"); *Altinex Inc. v. Alibaba.com Hong Kong Ltd.*, No. SACV1301545JVSRNBX, 2016 WL 6822235, at *12 (C.D. Cal. Mar. 25, 2016) (Alibaba acted "expeditiously" when listing was removed in same month as report); *Tiffany (NJ) Inc. v. eBay Inc.*, 600 F.3d 93, 99, 106 (2d Cir. 2010) (eBay terminated listings reported by mark holder "promptly," *i.e.*, "within twenty-four hours of receiving" notice).

3. Plaintiff Fails to Plausibly Allege that OpenSea Caused Him the Alleged "Permanent and Irreversible" Harm

Plaintiff's conclusory allegation that OpenSea's action (or alleged inaction) is the "direct and proximate cause" of "the theft and subsequent sale of" his NFTs (Compl. ¶ 134, ECF No. 1) also falls far short of the well-established standard for pleading proximate cause and, in fact, is contradicted by Plaintiff's own factual allegations.

"In tort actions," allegations "that a party other than the defendant caused the plaintiffs damages . . . negate an essential element of the plaintiff's claim—proximate cause." *Clark Cnty. Sch. Dist. v. Richardson Const., Inc.*, 168 P.3d 87, 96 (Nev. 2007). Courts routinely decide issues of proximate cause on the pleadings, particularly where the plaintiff alleges to have been harmed by the actions of a third party. *See, e.g.*, *Cardiello v. Venus Grp., Inc.*, 129 Nev. 1102 (2013) (unpublished disposition) (upholding dismissal without leave to amend when plaintiff alleged "that the auto accident that resulted in her injuries was caused by the negligence of the two drivers that rear ended her vehicle," not her employer's failure to carry workers' compensation insurance); *Bibicheff*, 844 F. App'x at 397 (upholding dismissal without leave to amend when alleged injury was result of third party's access to and unauthorized use of plaintiff's financial information, "for which PayPal is not alleged to have been responsible").

On Plaintiff's own allegations, OpenSea could not conceivably have prevented the harm Plaintiff alleges—loss of the "significant monetary value of the NFTs." (Compl. ¶ 114, ECF No. 1.) Plaintiff does not allege any harm other than the damages flowing directly from the theft itself, and such harm became "permanent and irreversible" the second the attacker transferred Plaintiff's NFTs into the attacker's own wallet. As Plaintiff explains, "individual NFT marketplaces do not have the ability to undo a transaction once it has been completed on the blockchain"—it becomes "permanent and irreversible" because "blockchain technology is decentralized and spread across thousands of computer nodes at various locations."[2] (*Id.* ¶ 4.)

[2] Plaintiff also alleges that the technical limitations on intervention—including intervention by

Because, as Plaintiff alleges, it is technically impossible to unwind the transfer of an NFT, Plaintiff was irreparably harmed the moment a third-party attacker took control of his NFTs—which took place immediately after Plaintiff clicked on the attacker's link to a fake "NFT Trader" website and the button to "approve the trade," before he contacted OpenSea customer service. (*See id.* ¶ 50.) Indeed, as Plaintiff acknowledges as to the two NFTs for which OpenSea disabled listings before resale using OpenSea, those NFTs were subsequently sold by the third-party attacker on another platform. (*Id.* ¶ 62 ("Following the freeze of the NFTs on OpenSea's marketplace," two "NFTs were later listed and resold on LooksRare.").) Because Plaintiff's "irreparable" loss had already occurred by the time the stolen NFTs were relisted on OpenSea, OpenSea cannot be deemed the proximate cause of Plaintiff's alleged injuries. *See, e.g.*, *757BD, LLC v. Nat'l Union Fire Ins. Co. of Pittsburgh, PA*, 804 F. App'x 592, 594 n.3 (9th Cir. 2020) ("It is axiomatic that X cannot be a proximate cause of Y if Y has already occurred before X."); *Aegis Ins. Servs., Inc. v. 7 World Trade Co., L.P.*, 737 F.3d 166, 179 (2d Cir. 2013) ("A defendant's conduct is not a cause-in-fact of an injury or loss if the injury or loss would have occurred regardless of the conduct.") (citing Prosser & Keeton, The Law of Torts § 41 (5th Ed. 1984).[3]

OpenSea indisputably did not directly or proximately cause a third party operating on an unaffiliated third-party Discord server and (fake) "NFT Trader" website to steal Plaintiff's NFTs, and all of Plaintiff's alleged harms flow directly from that theft. OpenSea's actions subsequent

---

law enforcement—are considered to be a "feature," rather than a "bug," of decentralized technology, and acknowledges it is at best "unclear" whether *even the FBI* could recover a stolen NFT. (*Id.* ¶ 21 ("Early enthusiasts have been drawn to cryptocurrencies and NFTs precisely because they enjoy the free-for-all atmosphere of NFT marketplaces, which offer a deregulated atmosphere that allows users to buy and sell NFTs free from banks, regulated stock markets, and the scrutiny of government agencies."); *id.* ¶ 59 ("[I]t is unclear whether the FBI can recover the stolen BAYC NFTs or stop their subsequent resells.").)

[3] For the same reason, even if Plaintiff was somehow further harmed by the subsequent resale of his NFTs—which he does not allege—OpenSea cannot be the proximate cause of such harm because two of the three NFTs were never resold using OpenSea and the third NFT could have been resold on LooksRare even if OpenSea had frozen it before it was resold using OpenSea.

to the "permanent and irreversible" harm caused by the theft could not possibly have reversed—let alone retroactively caused—such harm. *Clark Cnty. Sch. Dist.,* 168 P.3d at 96; *Bibicheff*, 844 F. App'x at 397.

B. Plaintiff's Substantively Duplicative Claims for Negligent Hiring and Negligent Training and Supervision Also Fail

Plaintiff's claims for negligent training and supervision (third cause of action) and negligent hiring (fourth cause of action) effectively re-plead his (deficient) claim for simple negligence. As noted above, OpenSea does not owe any duty to protect Plaintiff from harm caused by a third party, *see supra* section IV.A.1, and OpenSea was not the cause of Plaintiff's harm*, see supra* section IV.A.3. These duplicative claims should therefore also be dismissed.

Further, these claims are both facially inapposite because Plaintiff does not claim that OpenSea's employees directly caused his harm—only that their steps to remediate harm caused by a third party were inadequate. "To succeed on a claim for negligent hiring, training, supervision, and/or retention under Nevada law, a plaintiff must establish that: (1) defendant owed a duty of care to the plaintiff; (2) defendant breached that duty by hiring, retaining, training, and/or supervising an employee even though defendant knew or should have known *of the employee's dangerous propensities*; (3) the breach *caused the plaintiff's injuries*; and (4) damages." *Long v. Diamond Dolls of Nevada, LLC*, No. 3:19-CV-00652-LRH-CLB, 2020 WL 6381673, at *6-7 (D. Nev. Oct. 29, 2020) (emphases added) ("Employers have a general duty to conduct reasonable background checks on potential employees to ensure that they are fit for the position. *A breach occurs when an employer hires an employee even though the employer knew or should have known of that employee's dangerous propensities.*") (emphasis added and internal citation omitted).

"It is a basic tenet that for an employer to be liable for negligent hiring, training, or supervision of an employee, the person [causing the harm] must actually be an employee." *Rockwell*, 925 P.2d at 1181 n.5 ("When the cause of action is for negligent supervision, as opposed to respondeat superior, it does not matter if *the employee's actions* occurred within or

without his scope of employment.") (emphasis added). Further, "there must be evidence that the employer's negligence caused the alleged injury." *Chiles v. Underhill*, No. 03:05-CV-00179LRHRJJ, 2008 WL 822248, at *11 (D. Nev. Mar. 26, 2008) (even if employee had failed a psychological exam, there is no evidence that such failure was "in any way related" to the harm alleged); *see also Okeke v. Biomat USA, Inc.*, 927 F. Supp. 2d 1021, 1028 (D. Nev. 2013) ("Claims for negligent training and supervision are based upon the premise that an employer should be liable when it places an employee, who it knows or should have known behaves wrongfully, in a position in which the employee can harm someone else."); *Calove v. Nationstar Mortg.*, LLC, No. 2:14-CV-01329-JAD-NJK, 2015 WL 4508751, at *3 (D. Nev. July 24, 2015) (dismissing on the pleadings claim for negligent hiring and supervision when the plaintiff failed to name specific employees or allege facts showing it was plausible that the defendant had failed to conduct reasonable background checks).

Allegations that a defendant's employees *failed to protect* a plaintiff from harm caused *by a third party* do not state a claim for negligent hiring, training, or supervision. In one recent case, the District of Nevada cited *Rockwell* in dismissing a claim for negligent hiring, training, and supervision against Walmart because there was no evidence that the plaintiff's injury (from slipping on liquid on the floor) was caused by Walmart's employees. *Bock-Kasminoff v. Walmart, Inc.*, No. 2:20-CV-00949-JAD-EJY, 2022 WL 891448, at *3 (D. Nev. Mar. 24, 2022) ("Without evidence that Walmart was responsible for the liquid on the floor, [Plaintiff] can't" show that her "injury was caused by an employee who was negligently hired, trained, or supervised."). Courts have also specifically dismissed negligent hiring, training, and supervision claims that are premised on criminal attacks caused by third parties, as is the case here. *McLaren v. Hb Klub, LLC*, No. 07CVC1767, 2009 WL 8581696 (Ohio Com. Pl. Oct. 26, 2009) ("There is no evidence that an *employee's* act or omission proximately caused McLaren's injuries and that defendants' negligence in hiring and retaining their employees proximately caused the injuries. Instead, McLaren's injuries were caused by a third-party criminal attack off of the premises," which plaintiff alleged defendant's employees had failed to stop) (emphasis in original).

Plaintiff does not and cannot allege that *OpenSea's employees* stole his NFTs or in any way caused the third-party phishing attack that resulted in his injury. With respect to the negligent hiring claim, Plaintiff simply alleges that OpenSea and its employees "fail[ed] to hire a sufficient number of security and customer service employees who would safeguard and protect any and all NFTs" listed for sale "on their platforms" and that its employees "failed to monitor and verify the NFTs [listed for sale] on OpenSea's platform." (Compl. ¶¶ 160-162, ECF No. 1.) With respect to the negligent supervision and training claim, Plaintiff similarly alleges that OpenSea breached its duty "by not requiring employees to adhere to adequate and basic monitoring, verification, security, reporting, and response measures," that illegal sales of NFTs "cannot occur without knowledge, complicity, or negligence by OpenSea and LooksRare employees," and that OpenSea employees "failed to adequately verify, monitor, and respond to reports of improper and illegal sales." (*Id.* ¶¶ 152-153.) But OpenSea's employees had nothing to do with the alleged theft or the resulting "permanent and irreversible" harm—and acted promptly to disable listings of the NFTs when they were alerted about the alleged theft.

These allegations simply restate Plaintiff's negligence claim, and as shown by *Rockwell*, *Bock-Kasminoff*, and *McLaren*, allegations that OpenSeas employees failed to thwart harm caused by third parties are insufficient to state a claim for negligent hiring, training, or supervision. OpenSea has a duty to protect the public from harm caused *by its employees*—but *not* from harm caused by a third party as a result of the employee's alleged inaction. Plaintiff's claims for negligent hiring and for negligent training and retention should therefore be dismissed.

C. OpenSea's Terms of Service Contain a Broad and Enforceable Exculpatory Provision That Bars All of Plaintiff's Claims

Each of Plaintiff's claims also fails for a more fundamental reason: Plaintiff voluntarily accepted OpenSea's Terms of Service in the course of accessing his account and engaging in transactions, and his claims fall within the scope of the unambiguous exculpatory provision contained in the Terms of Service. This provision should be enforced to bar his claims.

1. Plaintiff Agreed to the Terms of Service

OpenSea publishes Terms of Service on its website. (Meader Decl. ¶ 3.) OpenSea periodically updates the Terms of Service, most recently on June 1, 2021 (the "June Terms"), and again on December 31, 2021 (the "December Terms"). (*Id.*) Both the June Terms and the December Terms state: "if you do not agree to these Terms, you may not access to use the Service." (*See id.*; *id.* Ex. A at 2.)

Plaintiff expressly agreed to the OpenSea Terms on multiple occasions, including when he purchased NFTs using OpenSea and used the mobile app for the first time. (Meader Decl. ¶¶ 6, 8; *see* Compl. ¶¶ 28-32, ECF No. 1 (alleging purchase of NFTs using OpenSea).) Specifically, before purchasing NFTs for the first time using OpenSea with a particular wallet, Plaintiff would have been required to check a box next to the statement that, "By checking this box, I agree to OpenSea's Terms of Service," which would have contained a hyperlink to OpenSea's Terms of Service. (Meader Decl. ¶ 5.) Plaintiff did this at least twice when the June Terms were in effect. (*Id.* ¶ 6.) Likewise, when Plaintiff used the OpenSea mobile app with a particular wallet for the first time, he would have been required to click a button underneath the statement: "By continuing, you agree to OpenSea's Privacy Policy and Terms of Service," which would have contained a link to the Terms. (*Id.* ¶ 7.) Plaintiff also did this at least twice when the June Terms were in effect. (*Id.* ¶ 8.)

"Courts throughout [the Ninth Circuit] circuit have consistently enforced agreements presented to users as clear, hyperlinked terms located near a required 'I agree' button, despite the agreement being imposed unilaterally on the user and the user not actually reading the terms." *My Daily Choice, Inc. v. Butler*, No. 2:20-CV-02178-JAD-NJK, 2021 WL 3475547, at *6 (D. Nev. Aug. 6, 2021) (enforcing terms "presented as a clear hyperlink near an 'I understand and agree to these policies and procedures' button"); *see also Spacil v. Home Away, Inc.*, No. 2:19-CV-00983-GMN-EJY, 2020 WL 184985, at *4 (D. Nev. Jan. 13, 2020) ("clickwrap agreements, which require the user to consent to terms and conditions by clicking a box on their computer screen before proceeding, are commonly upheld by the federal courts"); *Nguyen v. Barnes &*

Noble Inc., 763 F.3d 1171, 1176–77 (9th Cir. 2014) (courts have found "requisite notice for constructive assent where the browsewrap agreement resembles a clickwrap agreement—that is, where the user is required to affirmatively acknowledge the agreement before proceeding with use of the website"); *In re Facebook Biometric Info. Privacy Litig.*, 185 F. Supp. 3d 1155, 1166 (N.D. Cal. 2016) (user agreement enforceable where user had to "take some action—a click of a dual-purpose box—from which assent might be inferred."); *Magee v. WD Servs., LLC*, No. 2:16-CV-02132-JAD-VCF, 2017 WL 424857, at *2 (D. Nev. Jan. 30, 2017) (similar); *cf. Kai Peng v. Uber Techs., Inc.*, 237 F. Supp. 3d 36, 48 (E.D.N.Y. 2017) ("[C]ourts in this Circuit have upheld 'Sign–In Wrap' agreements where plaintiffs did not even click an 'I Accept' button, but instead clicked a 'Sign Up' or 'Sign In' button where nearby language informed them that clicking the buttons would constitute accepting the terms of service.").

Plaintiff likewise agreed to OpenSea's Terms of Service here.

2. The Terms of Service Unambiguously Bar Claims For Harm Caused By Unauthorized Third-Party Activities and for Negligence

Exculpatory provisions are "generally regarded as a valid exercise of the freedom of contract" and may be upheld to waive liability for alleged negligence when, as here, the exculpatory provision is unambiguous about whether it applies to claims for negligence. *Miller v. A & R Joint Venture*, 636 P.2d 277, 278 (Nev. 1981); *Waldschmidt v. Edge Fitness, LLC*, 417 P.3d 1120, 1120 (Nev. 2018) (unpublished disposition) (holding that "unambiguous exculpatory clause explicitly relieved respondent of liability" for negligence); *Kaufman*, 2020 WL 4251083, at *3 ("The exculpatory clause contained within the Agreement is clear and unambiguous and disclaims liability. . . . The exculpatory clause unambiguously identifies the parties' intent; and therefore, the Court has no authority to alter the terms of the Agreement."); *Laudisio v. Amoco Oil Co.*, 108 Misc. 2d 245, 247 (N.Y. Sup. Ct. 1981) (upholding provision that "clearly purports to absolve [defendant] from responsibility for 'its negligent acts or omissions'"); *Spancake v. Aggressor Fleet Ltd.*, No. 91 CIV. 5628 (DLC), 1995 WL 322148, at *3 (S.D.N.Y. May 26, 1995) (upholding provision "even if such claims arise out of the sole negligence" of defendant).

The OpenSea Terms of Service are clear and unambiguous. They identify the various risks associated with use of OpenSea and with the purchase, possession, and sale of NFTs more generally, and plainly state that by using OpenSea's services, the user agrees to assume all such risk. Specifically, the June Terms of Service include a disclaimer section stating that:

> **WE WILL NOT BE RESPONSIBLE OR LIABLE TO YOU FOR** ANY LOSS AND TAKE NO RESPONSIBILITY FOR, AND WILL NOT BE LIABLE TO YOU FOR, ANY USE OF CRYPTO ASSETS, INCLUDING BUT NOT LIMITED TO **ANY LOSSES, DAMAGES, OR CLAIMS ARISING FROM: .** . . (D) UNAUTHORIZED ACCESS OR USE; **(E) ANY UNAUTHORIZED THIRD PARTY ACTIVITIES, INCLUDING WITHOUT LIMITATION THE USE OF VIRUSES, PHISHING,** BRUTEFORCING OR OTHER MEANS OF ATTACK AGAINST THE SERVICE OR NFTS.

(Meader Decl. Ex. A at 11; Meader Decl. ¶ 3 (December Terms of Service contain substantially similar provision).)

The June Terms of Service also include an express limitation of liability section expressly providing that:

> TO THE FULLEST EXTENT PERMITTED BY LAW, **IN NO EVENT WILL OPENSEA BE LIABLE TO YOU OR ANY THIRD PARTY FOR ANY** LOST PROFIT OR ANY INDIRECT, CONSEQUENTIAL, EXEMPLARY, INCIDENTAL, SPECIAL OR PUNITIVE **DAMAGES** ARISING FROM THESE TERMS, THE SERVICE, PRODUCTS OR THIRD-PARTY SITES AND PRODUCTS, OR FOR ANY DAMAGES RELATED TO LOSS OF REVENUE, LOSS OF PROFITS, LOSS OF BUSINESS OR ANTICIPATED SAVINGS, LOSS OF USE, LOSS OF GOODWILL, OR LOSS OF DATA, AND **WHETHER CAUSED BY TORT (INCLUDING NEGLIGENCE), BREACH OF CONTRACT, OR OTHERWISE,** EVEN IF FORESEEABLE AND EVEN IF OPENSEA OR ITS SERVICE PROVIDERS HAVE BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES. ACCESS TO, AND USE OF, THE SERVICE, PRODUCTS OR THIRD-PARTY SITES AND PRODUCTS ARE AT YOUR OWN DISCRETION AND RISK, AND YOU WILL BE SOLELY RESPONSIBLE FOR ANY DAMAGE TO YOUR COMPUTER SYSTEM OR MOBILE DEVICE OR LOSS OF DATA RESULTING THEREFROM.

(Meader Decl. Ex. A at 12; Meader Decl. ¶ 3 (December Terms of Service contain substantially similar provision).)

Because the exculpatory provision "unambiguously identifies the parties' intent" to exculpate OpenSea for liability for harm caused by third-party conduct, including "phishing," and for any liability allegedly caused by negligence, "the Court has no authority to alter the terms of the Agreement." *Kaufman*, 2020 WL 4251083, at *3; *Agric. Aviation Eng'g Co. v. Bd. of Clark Cnty. Comm'rs*, 794 P.2d 710, 713 (Nev. 1990) (provision "show[s] the intent to release from liability beyond doubt by express stipulation," not "inference from the words of general import"). As all of the claims in this action arise from harm caused by "third party activities" including "phishing," and sound in negligence, the claims are barred by this provision.

3. The Exculpatory Provision Is Enforceable Against Plaintiff

The Terms of Service are enforceable because they do not contravene public policy and are not unconscionable as they "do[] not relate to essential services. [They] merely govern[] a voluntary [] activity. The signers are free agents who simply can walk away without signing the release and participating in the activity." *Cruz*, 2012 WL 7831781 ¶¶ 6, 9.

Courts in the Ninth Circuit have also consistently enforced limitation of liability clauses against users of websites for the same reason that the Nevada District Court enforced such a provision in *Cruz*—because the users are not required to use the service at issue. *See, e.g., Adkins v. Facebook, Inc.*, No. C 18-05982 WHA, 2019 WL 3767455, at *2 (N.D. Cal. Aug. 9, 2019) (holding that limitation of liability clause is not procedurally unfair even though it is a contract of adhesion and enforcing the clause because "plaintiff could have simply not enrolled in Facebook's social media service. Facebook is not a necessity of life and anyone who does not like the terms of service can go elsewhere"); *Darnaa, LLC v. Google, Inc.*, No. 15-CV-03221-RMW, 2015 WL 7753406, at *5 (N.D. Cal. Dec. 2, 2015) (noting that limitation of liability clauses "have long been recognized as valid in California" and enforcing such clause to bar claim for negligence notwithstanding argument that it is contrary to public policy, and even though there was "no dispute" that terms of service containing the clause were "a contract of adhesion"); *cf. Brozyna v. Niagara Gorge Jetboating, Ltd.*, No. 10-CV-602-JTC, 2011 WL 4553100, at *6 (W.D.N.Y. Sept. 29, 2011) (provision enforceable when "[t]he excursion 'is a

strictly voluntary recreational pursuit, and does not constitute the rendition of essential services'"); *Marine v. Macready*, 803 F. Supp. 2d 193, 201 n.6 (E.D.N.Y. 2011) (provision enforceable when "[n]othing in the record suggests that the college-educated Macreadys were prevented from reading the Lease Agreement . . . or from simply walking away").

Just as in *Cruz*, and just like users of Facebook and Google, Plaintiff was a "free agent[] who simply [could] walk away without" agreeing to the Terms of Service or using OpenSea. OpenSea is "not a necessity of life and anyone who does not like the terms of service can go elsewhere," including other NFT marketplaces. *See Adkins*, 2019 WL 3767455, at *2. The exculpatory provision is therefore enforceable and applies to bar all of Plaintiff's claims.

D. The Economic Loss Doctrine Also Bars All of Plaintiffs' Claims

All of Plaintiff's claims are also separately barred by the economic loss doctrine because they seek damages that are solely monetary in nature.

"Under the economic loss doctrine . . . economic losses are not recoverable in negligence absent personal injury or damage to property other than the defective entity itself." *Calloway*, 993 P.2d at 1267 (citing *Central Bit Supply v. Waldrop Drilling*, 717 P.2d 35, 36–37 (Nev. 1986) and *Local Joint Exec. Bd. of Las Vegas, Culinary Workers Union, Local No. 226 v. Stern*, 651 P.2d 637, 638 (Nev. 1982)); *see also Giles v. Gen. Motors Acceptance Corp.*, 494 F.3d 865, 879 (9th Cir. 2007) ("Broadly speaking, Nevada applies the economic loss doctrine to bar recovery in tort for purely monetary harm in product liability and in negligence cases unrelated to product liability.") "The primary purpose of the rule is to shield a defendant from unlimited liability for all of the economic consequences of a negligent act, particularly in a commercial or professional setting, and thus to keep the risk of liability reasonably calculable." *Stern*, 651 P2.d at 638. In addition to simple negligence claims, courts have applied the economic loss doctrine to bar negligent hiring, training, and supervision claims as well. *See Blanck v. Hager*, 360 F. Supp. 2d 1137, 1157-59 (D. Nev. 2005) (granting motion to dismiss negligent hiring, training, and supervision claim under Nevada law "based on the economic loss doctrine" as plaintiff "has not alleged personal injury, property damage, or intentional tortious behavior").

"The term 'economic loss' refers to damages that are solely monetary, as opposed to damages involving physical harm to person or property." *Giles*, 494 F.3d at 873 (analyzing Nevada's economic-loss rule). Here, Plaintiff's negligence claims fall squarely within the economic loss rule; his claimed damages are purely economic and do not involve any physical harm to person or property. Plaintiff claims that the theft of the BAYC NFTs "deprived [him] . . . of the significant monetary value of the NFTs he owned," as well as the "commercialization rights he possessed" in the NFT images and his "ability to earn future profits from his BAYC NFTs." (Compl. ¶¶ 114, 134, 143, 154, ECF No. 1.)[4] These are all plainly economic losses. *See id.*; *see also Calloway*, 993 P.2d at 1263 ("purely economic losses" include "consequent loss of profits, without any claim of personal injury or damage to other property"); *Redman v. John D. Brush and Co.,* 111 F.3d 1174, 1183 (4th Cir. 1997) (economic loss rule barred claims against safe manufacturer where coin collection of the plaintiff was stolen during a burglary from safe; "[t]he essence of [his] claim is that he suffered a loss because the safe did not function at the level he expected").

Accordingly, Plaintiff's claims should be dismissed as barred by the economic loss rule.

V. CONCLUSION

For the reasons set forth above, Plaintiff's claims against OpenSea should be dismissed without leave to amend.

[4] Plaintiff also vaguely and speculatively suggests that he has lost "membership in the BAYC community and the privileges associated with it." (*E.g.*, Compl. ¶ 154.) Plaintiff, however, nowhere defines what those privileges are and whether or why they might be non-economic in nature, and the complaint's allegations make clear that Plaintiff is focused on the alleged monetary loss from the stolen NFTs. At any rate, such conclusory and vague allegations are insufficient to overcome the economic loss rule. *See, e.g.*, *Closson v. Recontrust Co.*, No. 2:11-CV-00146-KJD, 2012 WL 893746, at *2 (D. Nev. Mar. 15, 2012) (holding that "statement of damages is too speculative and tangential" to "state a claim").

DATED this 3d day of June, 2022.

DICKINSON WRIGHT PLLC

/s/: Justin J. Bustos

JOHN P. DESMOND
Nevada Bar No. 5618
JUSTIN J. BUSTOS
Nevada Bar No. 10320
100 W. Liberty Street, Suite 940
Reno, NV 89501
Tel: (775) 343-7500
Fax: 844-670-6009
Email: jdesmond@dickinsonwright.com
Email: jbustos@dickinsonwright.com

MUNGER, TOLLES & OLSON, LLP
JONATHAN H. BLAVIN (Pro Hac Vice)
560 Mission Street, 27th Floor
San Francisco, CA 94105
Tel: (415) 512-4011
Email: Jonathan.Blavin@mto.com

ERIN J. COX (Pro Hac Vice)
BRANDON R. TEACHOUT (Pro Hac Vice)
APRIL D. YOUPEE-ROLL (Pro Hac Vice)
350 South Grand Avenue, Suite 5000
Los Angeles, CA 90071
Tel: (213) 683-9100
Email: Brandon.Teachout@mto.com
Email: Erin.Cox@mto.com
Email: April.youpee-roll@mto.com

Attorneys for Defendant Ozone Networks, Inc. d/b/a OpenSea, a New York Corporation

CERTIFICATE OF SERVICE

The undersigned, an employee of Dickinson Wright PLLC, hereby certifies that on the 3rd day of June 2022, I caused a copy of the foregoing **DEFENDANT OZONE NETWORKS, INC.'S MOTION TO DISMISS COMPLAINT** to be transmitted by electronic service in accordance the Court's CM/ECF e-filing system, addressed to:

Emily Brinn Nuvan (Pro Hac Vice)
Jose A. Abarca (Pro Hac Vice)
Romaine C. Marshall (Pro Hac Vice)
Armstrong Teasdale LLP
201 South Main Street, Suite 750
Salt Lake City, UT 84111
enuvan@atllp.com
jabarca@atllp.com
rmarshall@atllp.com

Attorneys for Plaintiff Robert Armijo

Michelle D. Alarie
Armstrong Teasdale LLP
3770 Howard Hughes Parkway, Suite 200
Las Vegas, NV 89169
malarie@atllp.com

Attorneys for Plaintiff Robert Armijo

John D. Tennert
Fennemore Craig, P.C.
7800 Rancharrah Parkway
Reno, NV 89511
jtennert@fclaw.com

Attorneys for Defendant Yuga Labs, LLC

Alison Clare Jordan
Fenwick & West LLP
801 California Street
Mountain View, CA 89041
Ajordan@fenwick.com

Attorneys for Defendant Yuga Labs, LLC

Samuel Sahagian (Pro Hac Vice)
Jennifer C. Bretan (Pro Hac Vice)
Katherine A. Marshall (Pro Hac Vice)
Michael S. Dicke (Pro Hac Vice)
Fenwick & West LLP
555 California Street, 12th Floor
San Francisco, CA 94104
ssahagian@fenwick.com
jbretan@fenwick.com
kmarshall@fenwick.com
mdicke@fenwick.com

Attorneys for Defendant Yuga Labs, LLC

/s/: Dianne M. Kelling
An Employee of Dickinson Wright PLLC